IBM Italy News Room

IBM Security annuncia App Exchange per promuovere la collaborazione contro il cybercrime

I partner offrono nuove app di security analytics basate su QRadar e sviluppate utilizzando strumenti di programmazione open

Milano - 10 dic 2015: IBM ha annunciato di aver reso 'open' la piattaforma di analytics per la sicurezza, IBM Security QRadar, per permettere a clienti, business partner e sviluppatori di realizzare app personalizzate sfruttando le funzionalità di security intelligence. IBM annuncia anche Security App Exchange, un marketplace a disposizione della community di esperti in sicurezza per creare e condividere app basate sulle tecnologie IBM. L'apertura della piattaforma di security analytics rappresenta il secondo passo importante, compiuto da IBM quest'anno, per promuovere la collaborazione e l'innovazione nel settore con l'obiettivo di combattere il cybercrime organizzato. Lo scorso aprile IBM ha reso disponibile il proprio database di minacce alla sicurezza, contenente 700 TB di dati, tramite IBM X-Force Exchange,una piattaforma di condivisione delle minacce informatiche alla quale hanno già aderito più di 2.000 aziende. Con l'annuncio della piattaforma di security analytics in aggiunta al database di intelligence sulle minacce, IBM intende promuovere una maggiore collaborazione nel settore consentendo alle organizzazioni di condividere sia i dati sia le competenze per combattere i cyber-criminali.

IBM e partner quali Bit9 + Carbon Black, BrightPoint Security, Exabeam e Resilient Systems hanno già popolato IBM Security App Exchange con decine di app personalizzate, che estendono la security analytics di IBM Security QRadar in ambiti quali il comportamento degli utenti, i dati degli endpoint e la visualizzazione degli incidenti. Queste nuove app sfruttano le nuove interfacce di programmazione applicative (API) open source di QRadar,la piattaforma di security intelligence di IBM che utilizza data analytics e threat intelligence allo scopo di rilevare gli incidenti di sicurezza per le migliaia di security operation center diffusi in tutto il mondo.

"Con migliaia di clienti che già stanno adottando tecnologie di sicurezza IBM, l'apertura di questa piattaforma per una più stretta collaborazione e lo sviluppo con partner e clienti cambia oggi l'economia della lotta al crimine informatico", spiega Marc van Zadelhoff, Vice President, Strategy and Product Management, IBM Security. "La condivisione delle competenze nel settore della sicurezza ci permetterà infatti di innovare più rapidamente, per avere la meglio su attacchi sempre più sofisticati".

Le nuove applicazioni velocizzano l'accesso agli analytics

Sviluppo e collaborazione aperti rappresentano uno strumento essenziale per accelerare l'innovazione nel panorama tecnologico attuale, in rapida evoluzione. Più del 77 percento dei responsabili aziendali afferma che le prassi di sviluppo collaborativo hanno apportato un beneficio alle rispettive organizzazioni, grazie ad un ciclo di sviluppo dei prodotti più breve e a un più rapido time-to-market[i].

Decine di organizzazioni hanno aderito all'IBM App Exchange, che ha già favorito la condivisione di 14 nuove applicazioni QRadar da parte di sviluppatori IBM e partner quali Bit9+Carbon Black, BrightPoint Security, Exabeam e Resilient Systems. Altri partner come STEALTHbits e iSIGHT Partners stanno sviluppando ulteriori app.

Grazie all'integrazione con le tecnologie di terze parti, queste nuove app sono progettate per offrire alle aziende una migliore visibilità su varie tipologie di dati e nuove funzioni automatizzate di ricerca e reporting, per aiutare gli specialisti della sicurezza a focalizzarsi sulle minacce più urgenti. Le app disponibili gratuitamente tramite l'IBM App Exchange, consentono alle aziende di accedere a un' ampia varietà di analytics integrati nell'ambiente di security intelligence di IBM QRadar.

Alcuni esempi di queste nuove applicazioni:

- **User Behaviour** – L'app Exabeam User Behavior Analytics integra gli analytics comportamentali a livello utente e il profilo di rischio direttamente nel dashboard di QRadar. Questa vista in tempo reale del rischio utente permette alle aziende di rilevare sottili differenze di comportamento tra un dipendente e un hacker che utilizza le stesse credenziali.
- **Threat Intelligence** - Una nuova app sviluppata da IBM consente agli utenti di QRadar di estrarre feed di threat intelligence utilizzando lo standard aperto STIX e i formati TAXII e di utilizzare questi dati per creare regole personalizzate per la correlazione, la ricerca o il reporting. Ad esempio, gli utenti potrebbero importare da IBM X-Force Exchange raccolte pubbliche di indirizzi IP pericolosi e creare una regola per aumentare il livello di rischio degli incidenti che comprendono indirizzi IP provenienti da tale lista.
- **Endpoint Detection and Response –** Una nuova app di Bit9 + Carbon Black fornisce agli utenti di QRadar una visibilità più approfondita delle minacce su dispositivi, desktop, laptop e server terminali. Analizzando i dati dei sensori degli endpoint dall'interno dell'interfaccia di QRadar, la Carbon Black App for IBM QRadar permette ai clienti di rilevare e rispondere agli attacchi sferrati agli endpoint più rapidamente.
- **Incident Visualization –** La nuova IBM Security QRadar Incident Overview App consente agli utenti una migliore visualizzazione di tutte le infrazioni all'interno della rispettiva installazione QRadar, utilizzando bolle, colori e linee di correlazione. Le dimensioni e il colore della bolla indicano l'entità dell'incidente, mentre le linee tracciate tra le bolle indicano indirizzi IP condivisi tra gli incidenti collegati. Questo approccio di visualizzazione intuitivo consente agli analisti della sicurezza di identificare rapidamente gli elementi comuni tra gli incidenti e di definire meglio la priorità di quelli importanti.

Queste applicazioni sono supportate dal nuovo framework applicativo di QRadar, che permette di creare rapidamente nuove applicazioni QRadar tramite API open e kit di sviluppo. IBM Security eseguirà test rigorosi di ogni applicazione prima della pubblicazione su App Exchange, per assicurare l'integrità dei contributi della community.

IBM Security QRadar velocizza le ricerche e risponde automaticamente alle minacce

IBM annuncia inoltre una nuova release di IBM Security QRadar, che analizza i dati su tutta l'infrastruttura IT di un'organizzazione al fine di individuare le potenziali minacce alla sicurezza. IBM è leader di mercato nel Security Information and Event Management (SIEM) in termini di revenue software del 2014, e ha mantenuto la posizione di leadership nel Magic Quadrant di Gartner per il SIEM negli ultimi 7 anni.

Per la prima volta, QRadar permetterà ai clienti di creare regole che interverranno automaticamente al rilevamento di specifiche minacce. Le regole create all'interno di QRadar possono, ad esempio, bloccare automaticamente gli indirizzi IP e controllare l'accesso degli utenti, sulla base del rispettivo profilo di rischio. Inoltre, le applicazioni sviluppate mediante il nuovo framework applicativo di QRadar possono sfruttare regole personalizzate, per rispondere automaticamente alle minacce.

IBM sta integrando QRadar con la gestione della sicurezza degli endpoint IBM BigFix, per aiutare le aziende a definire meglio le priorità delle minacce e le patch sui dispositivi degli utenti. QRadar è ora in grado di individuare gli endpoint esposti che non hanno BigFix installato, aiutando le aziende a rilevare più rapidamente gli asset illegali o non gestiti.

IBM Security
La piattaforma IBM per la sicurezza mette a disposizione delle organizzazioni la security intelligence necessaria a proteggere in modo completo persone, dati, applicazioni e infrastrutture. IBM offre soluzioni per la gestione delle identità e degli accessi, gestione delle informazioni e degli eventi di sicurezza, sicurezza del database, sviluppo applicativo, gestione del rischio, gestione degli endpoint, protezione dalle intrusioni di prossima generazione e molto altro ancora. IBM gestisce una delle più vaste organizzazioni al mondo di ricerca e sviluppo e di delivery in materia di sicurezza. Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il blog di IBM Security Intelligence.

Disclaimer: *Le dichiarazioni di IBM riguardanti i programmi, le indicazioni e gli intenti futuri sono soggette a modifica o ritiro senza preavviso, ad esclusiva discrezione di IBM. Nelle decisioni di acquisto non si deve fare affidamento sulle informazioni riguardanti i potenziali prodotti futuri, che sono intese unicamente a delineare l'indirizzo generale dei nostri prodotti. Le informazioni citate riguardanti i potenziali prodotti futuri non costituiscono un impegno, una promessa o un obbligo giuridico a fornire materiali, codici o funzionalità. Le informazioni sui potenziali prodotti futuri non possono essere incorporate in alcun contratto. Lo sviluppo, il rilascio e la tempistica delle caratteristiche o funzionalità future, descritte per i nostri prodotti, restano a nostra esclusiva discrezione.*

Gartner disclaimer: *Gartner non sostiene alcun fornitore, prodotto o servizio descritto nelle sue pubblicazioni di ricerca e non consiglia agli utenti di tecnologia di scegliere solo i fornitori con le valutazioni più alte. Le pubblicazioni di ricerca di Gartner sono costituiti dai pareri di istituti di ricerca Gartner e non devono essere interpretate come dichiarazioni di fatto. Gartner non riconosce alcuna garanzia, espressa o implicita, relativamente a questa ricerca, inclusa qualsiasi garanzia di commerciabilità o idoneità per uno scopo particolare*.

---

[i] *Linux Foundation Collaborative Trends Report 2014*.
